~~TOP SECRET~~

ARMED FORCES SECURITY AGENCY

99/50/TOPSEC/AFSA-14

Copy No. 33

From: AFSA-14

To: _____

~~TOP SECRET~~

DF 217

99/50/TOPSEC/AFSA-14

THE RUSSIAN CIPHER DEVICE K-37

1. The attached is an Armed Forces Security Agency translation of a paper by Dr. Grimmsen entitled: "Russisches Chiffriergerät K 37" recently forwarded by Headquarters, Army Security Agency, Europe.

2. Apparently Dr. Grimmsen made a careful study of this machine based on one captured early in the war.

3. Attention is called to the study of the K 37 already translated and issued as DF 74.

September 1950

Translated: WJH

Distribution: Normal

35 copies

12 pages

DF 217

The Russian Cipher Device K-37

Time of Examination: 1942

Summary:

A. Cryptographic-Technical:

1) Hagelin patent, corresponding to the French machine B-211 with certain changes.

2) Cryptographic security only conditionally sufficient.

B. Technical:

Well built throughout from the point of view of construction, mechanically such clean work that it is probable that the device is not of Russian manufacture. The contrary, however, cannot be proven.

C. Operational:

The device is just being introduced and has been issued to some offices of the Russian Army but not yet put into use (report dated September 1941). The device is supposed to replace all other cryptographic systems. (Up to this point the Russian Army probably used only hand systems).

DF 217

The Russian Cipher Device K-37

The device is intended for enciphering plain text and for converting enciphered text into plain text. By striking the keyboard, the enciphered or deciphered text is printed on a narrow roll of paper.

Illustration 1 shows a complete view of the apparatus, illustration 2 the inside view.

The keyboard (1) contains 30 letter keys and 1 space key. The letter keys work together with 11 selector bars which lie under the keys and which are divided into two groups of 5 and 6 selector bars each. Let us designate the groups as R and S. The keys are coordinated with the selector bars in such a way that the pressing of a key activates one R and one S bar. Each bar is provided with a contact which when closed excites a magnet (3). Correspondingly there are also two groups of magnets, i. e., 5 + 6 = 11 magnets. An additional magnet is assigned to the spacing function. Each magnet for its part effects the adjustment of a selector ring in the printer (4). The selector rings (not visible in the illustration) have notches which are so arranged that with a movement of one selector ring each from the R and S groups one of the 30 draw bars is released. It then snaps forward under the influence of a spring and in doing so its front end arrives in the path of a rotating stop. This stop is fastened to a type wheel which is driven by means of a friction coupling and thus at the forward snap of a draw bar is held at a certain position. Like the 30 draw bars the type wheel (5) can be held at 30 different positions and for that reason it contains 30 characters.

Each time a key is pressed, then via the roundabout way of magnet activation a character is printed. Which character is printed depends upon the association of the selector bars to the magnets. The encipherment is effected by the transposition of the electrical connections between these two elements. The transposition can therefore be undertaken only within the two groups R and S, for only so is there a guarantee that at each striking of a key an R and an S magnet will be excited, which condition, as we have seen, must be fulfilled for the printing of this character.

DF 217

In order to carry out the transposition, there are two wheel switches (6 and 7) with 5 and 6 current paths respectively. They have 10 and 12 settings respectively so that there can be 10 and 12 different associations respectively, e. g.

	First group	Second group
Key contacts	A B C D E F	A B C D E
Magnets	A B C D E F	A B C D E

The external structure of the wheel switches can be seen in illustration 3, the wiring in illustration 4. On its disc-shaped part the wheel has 10 or 12 contacts a, as the case may be, of which two are always connected one with the other and with a collector ring b. Standing opposite the 10 or 12 contacts a are 5 or 6 spring contacts c (hereafter called "brushes"). The lead to the collector rings proceeds via the collector springs d.

The two switch wheels are advanced independently of one another by a set of wheels with adjustable pins, which is reproduced schematically in illustration 5. For each wheel switch there are 2 pin wheels a and b. These have 29, 27, 23 and 19 adjustable pins. When the adjustable pins are in "+ position", they engage a small intermediate wheel c and thereby advance the switch wheel d by one position. This forward movement therefore occurs when one of the two associated switch wheels, or both simultaneously, engages a pin which is in + position. The leads to the 11 selector bar contacts, to the 11 magnets and to the 22 inlets and outlets of the wheel switches are all gathered together in a cable which terminates in a multiple plug. The matching plugbox (which was missing in the machine examined) is obviously connected to a switch system which allows any desired association of the contacts, magnets and switch wheel inlets within the R and the S groups. (Supplemental change of wiring!)

By means of a mechanical switch the set of pin wheels can be uncoupled so that the wheels can be reset independently of one another. The switch has four positions and in addition to coupling the set of wheels it also causes the following changes:

DF 217

1) Position "Т"*, probably "testing".

The set of wheels is uncoupled. Key Й and the space key can be activated. The latter always yields a space by exciting the space magnet.

2) Position "З",* probably "encipherment".

Key 1 is blocked. The space key yields a character according to the encipherment. The enciphered text is divided into groups of four.

3) Position "Р",* probably "decipherment".

Key 1 is open. The space key is blocked. Continuous text is printed. A space appears instead of the character Й.

4) Position "З-Р".* Purpose unclear. The space key is blocked, key 1 is open. Division into groups of four.

The device is of slight weight and has small dimensions (275 x 275 x 135 [centimeters]). It makes very little noise. The workmanship of the parts is very neat, but many parts seem too tiny for use under field conditions. The support of the switch wheels is especially precarious. Power is furnished by a 24-volt direct current motor.

Cryptographic-Technical Examination

Diagram 1 shows the scheme of encipherment. On the left-hand side the keyboard is represented, and here the Cyrillic letters have been replaced by Latin letters. Next to it and below it are the matching key contacts A to F

---

* Translator's note: In these four cases it is believed that in the German text the characters in quotes were attempts to represent the Cyrillic alphabet while using a typewriter with only Latin letters. Consequently these letters appear in this translation in their Cyrillic form. The original Latin and the Cyrillic characters along with their probable expansions are as follows:

1) "Т", "Т", ТЕКСТ = text [plain]; 2) "З", "З", ЗАШИФРОВАНИЕ = encipherment; 3) "Р", "Р", РАСШИФРОВАНИЕ = decipherment; and 4) the combination of 2) and 3) above. Support is lent to this belief by the fact that in paragraphs describing 1) and 3) was represented by a Latin N with a breve above it. In addition, at least on some Russian typewriters the same character is used to represent both the digit 3 and the Cyrillic letter З.

(group S in black) and A to E (group R in red). From the central section of the diagram it is possible to see the function of the two wheel switches. The "brushes" I to V and I to VI are always connected with the "collector rings"(1 to 5 and 1 to 6) which are inserted in a vertical column.

The 10 and 12 vertical columns correspond to the 10 and 12 settings of the two switch wheels. The "brushes" are linked with the key magnets, likewise the "collector rings" with the magnets A to E and A to F. The right side of diagram 1 shows the association of the characters to the magnets.

In deciphering the reverse holds true; the key contacts are linked with the collector rings and the magnets with the brushes. (Naturally it is also possible to encipher with this second wiring and to decipher with the first).

From the diagram we can see that the sequence of the collector rings is the same for each brush, only the start of the sequences is different. Since the collector rings are associated with certain magnets and the brushes with certain contacts, we can therefore substitute in the diagram for the numbers the letters of the magnets and contacts. We then find in the following example:

Contacts	Magnets
E	B E D F C B A D F C E A
A	E A B E D F C B A D F C
F	F C E A B E D F C B A D
D	A D F C E A B E D F C B
B	C B A D F C E A B E D F
C	D F C B A D F C E A B E

From the diagram we can see that it suffices to obtain a vertical and a horizontal line in order to determine the whole diagram, i. e., the whole key. Because of the fact that the switch wheel is not moved forward at every character struck, the switch sequence is changed in such a way that the vertical columns are repeated, e. g.

DF 217

Contacts	Magnets
E	B E E D F F F F C B A D D D F F C E E E A
A	E A A B E E E E D F C B B B A A D F E E C
F	F C C E A A A A B E D F F F C C B A A A D
D	A D D F C C C C E A B E E E D D F C C C B
B	C B B A D D D D F C E A A A B B E D D D F
C	D F F C B B B B A D F C C C E E A B B B E

If there is a "compromised text", i. e., if we have a piece of plain text and the matching cipher text, then we also know the sequence of the contacts and magnets, e. g.:

(Group S)

Contacts	C A D B B E F E A C B F E E D
Magnets	A C B F D F A D B A E B D D E

The underlined positions give the first clue. The arrangement of the switch wheel of group S shows no position where the same magnet acts twice in succession. The magnet sequence DD for the contact sequence EE must therefore be due to a standstill of the switch wheel. Conversely at the position where the magnet sequence FD appears for the contact sequence BB there must have been a forward movement.

The number of teeth of the pin wheels are known (19 and 23). Since a standstill occurs only when at this position both wheels have a "standstill position", i. e., no advancing pin, we know that "standstill" is again produced after 19 steps by the one wheel and after 23 steps by the other wheel. If despite this fact at such a position an advance has occurred, then this must be due to the other wheel. We have thus obtained an "advancing pin". Taking into account the peculiarities of the magnet sequences as given by the known wiring of the switch wheel, it becomes easily possible with about 150 letters of compromised text to obtain the pattern of the pin wheels and the association of the magnets to the contacts. If by chance we find rather long sequences of identical contacts which hit on a rather long standstill period, the text required can be much shorter. To determine the group R is more difficult in that, because of the particular wiring of the switch wheel, even where there is stepping the same magnet is switched on twice in succession

DF 217

(see illustration 4, contacts e). Despite this we do reach our goal by experimentally associating in succession each of the five magnets with the double contact. Here the false assumptions lead to contradictions so that the correct association is left as the only possible one.

Schlüsselgerät K 37, 1942

Abb 1

Abb. 2

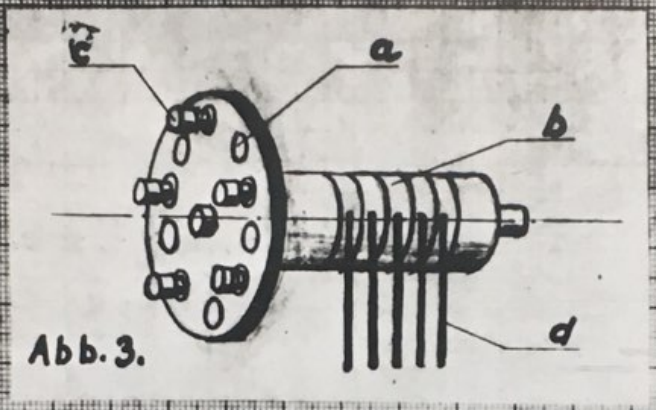


Abb. 3.

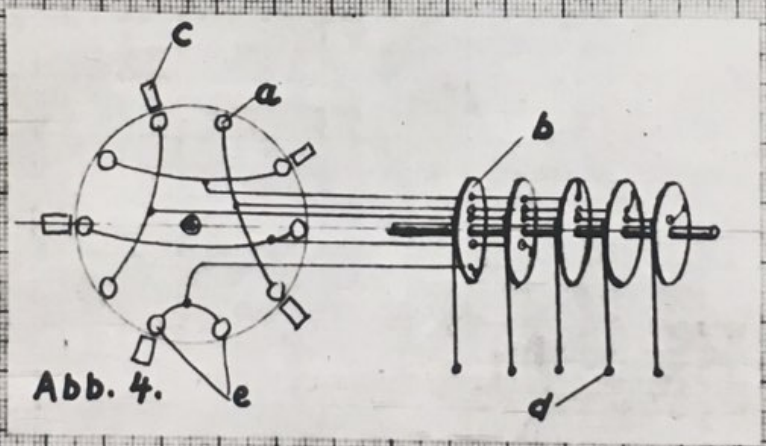


Abb. 4.

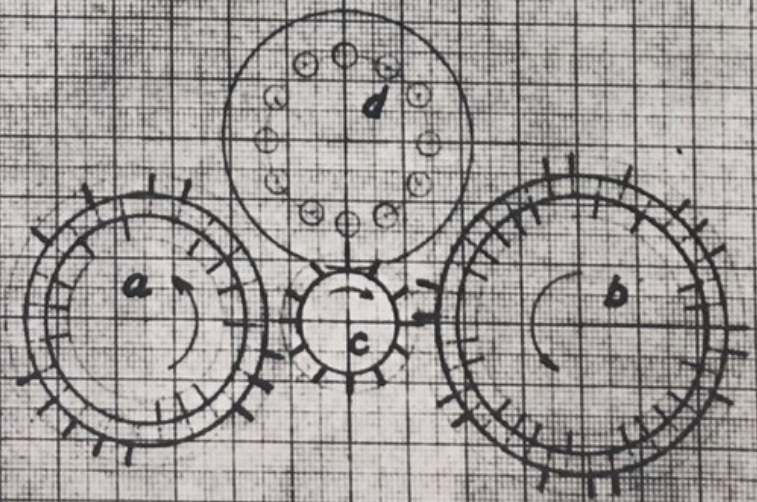
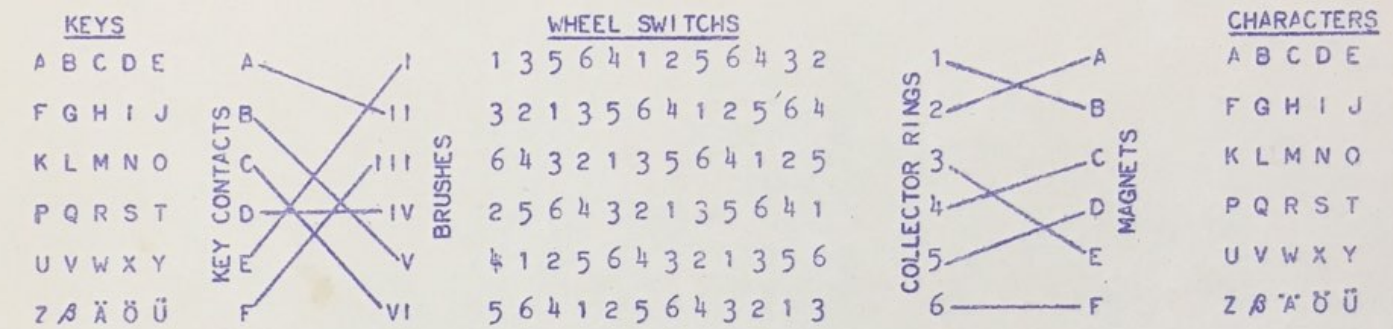
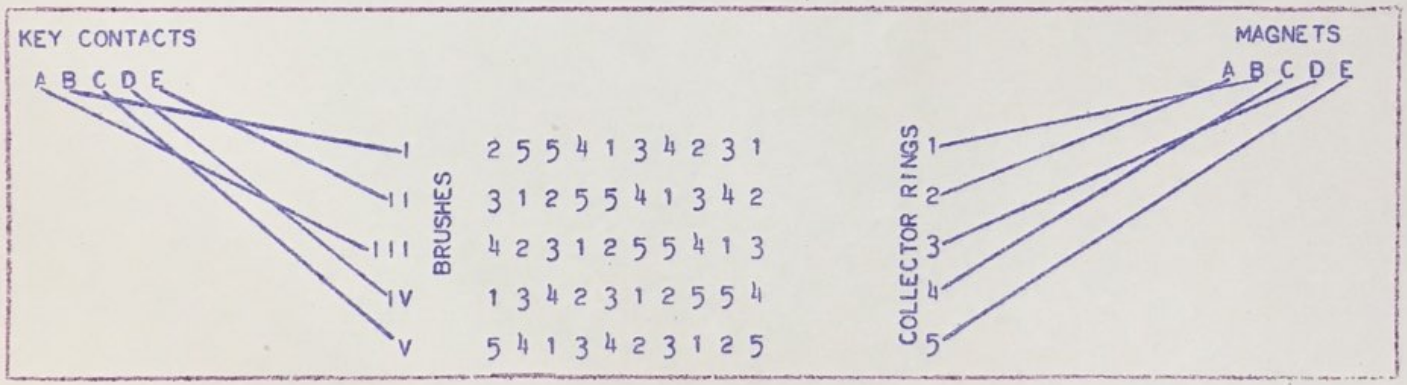


Abb. 5.

DF-217

DIAGRAM 1





THE SWITCH SETTING INDICATED BY ARROWS HAS, FOR EXAMPLE, THE FOLLOWING CONNECTION:

KEY CONTACT A - BRUSH II - COLLECTOR RING 3 - MAGNET E) KEY A THUS PRINTS
[illegible] E) CHARACTER Y.

OR

" " C - " VI - " " 1 - " B) KEY N THUS PRINTS
[illegible] A) CHARACTER F.

TOP SECRET